Сигурносни препораки на Интернет банката на Комерцијална банка АД Скопје за спречување на измами со злоупотреба на идентитет

"Синџирот е онолку силен, колку што
е силна неговата најслаба алка"

Почитувани корисници,

Потребата да се докаже сопствениот идентитет е составен дел на модерното живеење. Во светот трендот на криминални дела кои во себе вклучуваат злоупотреба на украден или непостоечки идентитет е во пораст. Документот објаснува што можете да сторите Вие лично се со цел да спречите криминален обид за кражба на вашиот идентитет односно негова злоупотреба и дополнително нуди совети кои можат да ви помогнат во хипотетичка ситуација во услови кога се сомневате дека сте жртва на кражба на вашиот идентитет.

Во брошурата која можете да ја симнете од сајтот на Интернет банката се дадени сигурносни препораки за корисниците на Интернет банката произлезени од најдобрата светска пракса на полето на информативната сигурност (best security practices).

ЗАБЕЛЕШКА: Во случај на било какво невообичаено однесување на интернет прегледувачот, при користењето на Интернет банката на Комерцијална банка, што може да биде последица на евентуални злонамерни програми инсталирани на вашиот компјутер (virus, trojan, spyware...), ве молиме што поскоро да го контактирате нашиот Help Desk, да го информирате за настанатата ситуација и да ги следите сигурносните препораки кои при тоа ќе ги добиете.

Сигурносни препораки на Интернет банката на Комерцијална банка АД Скопје за спречување на измами со злоупотреба на идентитет

Содржина

Корисниците на Интернет банката и нивната улога во сигурносниот систем

Најпрвин да појасниме дека од пионерските почетоци на отпочнувањето на работата на Интернет банката на Комерцијална банка во 2001 год., отпочнувањето на пилот продукцијата за вршење на плаќања во домашниот платен промет за правни лица во септември 2004 год. како и отпочнувањето на масовната продукција на 1 откомври 2006 па се до денес, ниту еден корисник (правно или физичко лице) на Интернет банката не пријавил, ниту бил жртва на неовластен пристап до информациите на банкарските сметки со кои располага (личните или сметките на компанијата во чие име работи) ниту пак е зебележан инцидент на неовластено располаѓање на средствата на сметките преку услугите на Интернет банката.

Дополнително во периодично спроведените ethical hacking тестирања од страна на домашни и странски компании специјализирани на полето на информативната сигурност, не се забележани слабости кои би можеле сериозно да ја загрозат сигурноста на Интернет банката како во изборот и примената на технологиите така и во востановените процеси и активности на лицата задолжени за нејзиниот развој и одржување.

Независно од сите континуирани и сихронизирани напори на полето на сигурноста што ги прави Развојниот тим на Интернет банката со Тимот за информативна сигурност и Одговорниот за сигурноста на информативниот систем на Банката како и другите стручни лица и служби во рамките на Банката, сигурноста од секогаш била прашање на идеално избалансиран спој на врвно обучен кадар, добро информирани и обучени корисници, избор и примена на сигурни и светски признати технологии како и нивна секојдневна употреба низ добро дефинирани процедури и низа заштитни мерки препознаени под терминот best security practices.

Се со цел традицијата на сигурно користење на Интернет банката да продолжи и во иднина, овој документот е посветен на најважната алка во синџирот на сигурносниот систем на Интернет банката, токму на оние за чија заштита истиот е имплементиран: нашите ценети корисници без кои сигурносниот систем независно од имплементираните технички контроли и процеси би можел да биде доведен во прашање доколку истите не обрнат внимание на одредени закани кои за жал постојат при секојдневното користењето на Интернетот.

Кражба на идентитетот и измама со злоупотреба на идентитетот

Кражба на идентитетот (Identity theft) е користење и злоупотреба на идентитетот на друга личност без нејзино знаење и одобрување. Измамникот мора да добие пристап до вашите лични податоци или да ги украде вашите документи за лична идентификација независно дали истите се во хартиена форма (лична карта, патна исправа) или се работи за дигитални белези за утврдување на вашиот идентитет како што се вашето корисничко име и лозинка, листа или уред за генерирање на кодови за еднократна употреба, вашиот дигитален сертификат складиран на PC, CD или сигурносен токен, PIN-от за пристап до дигиталниот сертификат итн.

Измама со злоупотреба на идентитет (Identity fraud) представува неовластено користење односно злоупотреба на украден идентитет во криминални активности чија крајна цел е противправно стекнување на добра, услуги или финансиски средства.

Бидете секогаш внимателни - Социјален инженеринг

Социјален инженеринг претставува софистицирано манипулирање со дадена личност од страна на измамникот се со цел истиот од жртвата неавторизирано да извлече чувствителни информации или да ја увери жртвата да изведе низа од неавторизирани активности.

Наместо измамникот да се обидува да ги пронајде и да ги искористи евентуалните слабости во техничките контроли на информативниот систем и лично да пенетрира со примена на софистицирани хакерски техники и алатки, истиот се обидува да воспостави однос на доверба со жртвата и ставајќи ја во заблуда во поглед на својот идентитет, жртвата ја манипулира се со цел да ги украде чувствителните информации кои понатаму би биле искористени во други криминални дела. Најчесто измамникот се претставува со лажен идентитет фалсификувајќи ја e-mail адресата на испраќачот и користејќи го заштитното лого на компанијата во чие име сака да се претстави но за целите на социјалниот инженеринг можат да бидат искористени и многу поконвенционални средства на комуникација како што се телефонот и поштата.

Препораки

Никогаш не ги давајте вашите лични податоци или финансиски информации (вашите сметки на пример) на непознати личности кои ве контактираат од компании со кои никогаш не сте комуницирале претходно а ве контактираат по пат на електронска пошта, телефон или писмено. Дополнително истото важи и за агенциите кои се претставуваат како консултанти, извршители или маркетинг агенции на компанија со која веќе имате воспоставено деловен однос најмалку заради фактот што немате никаква гаранција за идентитетот на третата страна која бара пристап до чувствителните информации.

Имајте го во предвид фактот дека ваквите контакти од некоја трета страна (агенција) во име на Банката се малку веројатни. Согласно Законот за заштита на личните податоци и интерните акти на Банката без ваша писмена согласност ниту една ваша контакт информација како што е тел. број, вашата e-mail адреса или вашата домашна адреса не смее да биде дадена на трета страна (агенција, друга компанија и сл.).

Согласно Политиката за информативна сигурност на Банката како и Упатството за примена на Политиката за информативна сигурност ниту едно службено лице од Банката ниту пак некоја трета страна со која Банката има склучено договор за соработка, никогаш, независно од ситуација заради која ве контактира не смее да побара да му ги разоткриете следните дигитални белези за идентификација за пристап на сервисите на Интернет банката:

- вашата корисничка лозинка;
- пинот за пристап до вашиот дигитален сертификат, и
- листата на кодови за ендократна употреба

Независно дали лицето ве контактира по телефон, електронска пошта и дали се обидува да ви помогне во отстранувањето на даден технички проблем за кој во моментот можеби Вие сте побарале помош, доколку погоре наведениот инцидент се случи веднаш прекинете ја комуникацијата со тоа лице и известете го Help Desk-от на Банката за настанот.

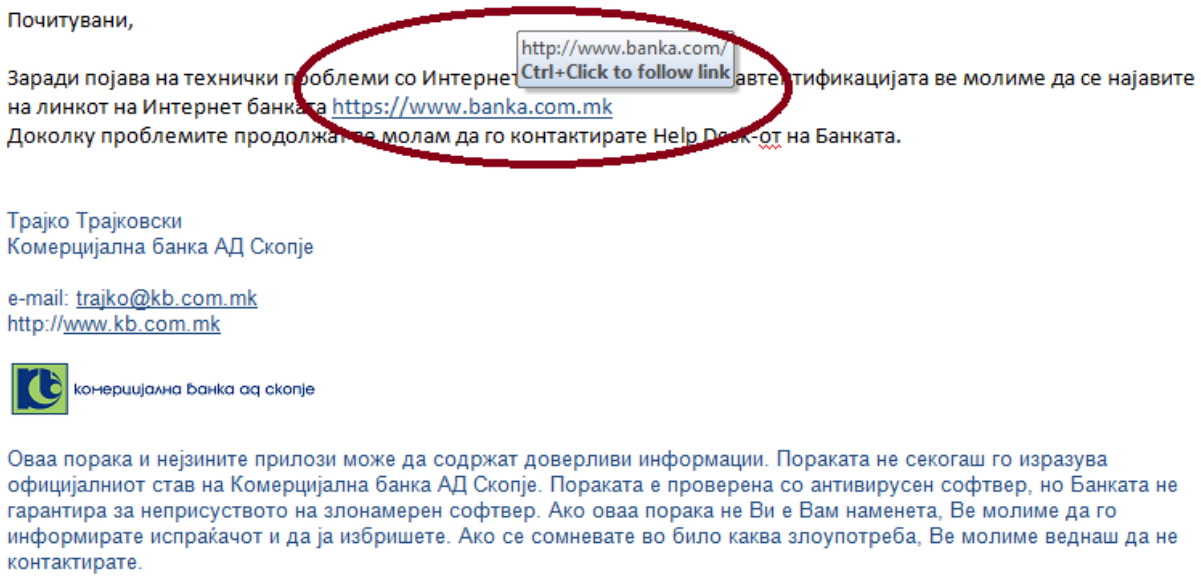
Внимавајте да не ве уловат - Риболов (Phishing)

Phishing **-** от е добро осмислена измама чија крајна цел е прибирање на чувствителни информации најчесто дигитални белези за лична идентификација како кориснички имиња и лозинки, PIN-ови за картички или PIN-ови за пристап до дигиталниот сертификат при што измамникот се маскира се со цел да наликува на доверливиот ентитет во електронската комуникација со кој корисникот е навикнат да работи (на

пример сајт кој наликува на Интернет банката на Комерцијална банка АД Скопје).

Риболов со помош на пораки пратени по електронска пошта

Еден класичен обид за измама во која се комбинира социјалниот инженеринг и риболовот како техника би бил следниот пример:


Почитувани,

Заради појава на технички проблеми со Интернет
http://www.banka.com/
Ctrl+Click to follow link
авте тификацијата ве молиме да се најавите на линкот на Интернет банката https://www.banka.com.mk
Доколку проблемите продолжат ве молам да го контактирате Help Desk-от на Банката.

Трајко Трајковски
Комерцијална банка АД Скопје

e-mail: trajko@kb.com.mk
http://www.kb.com.mk

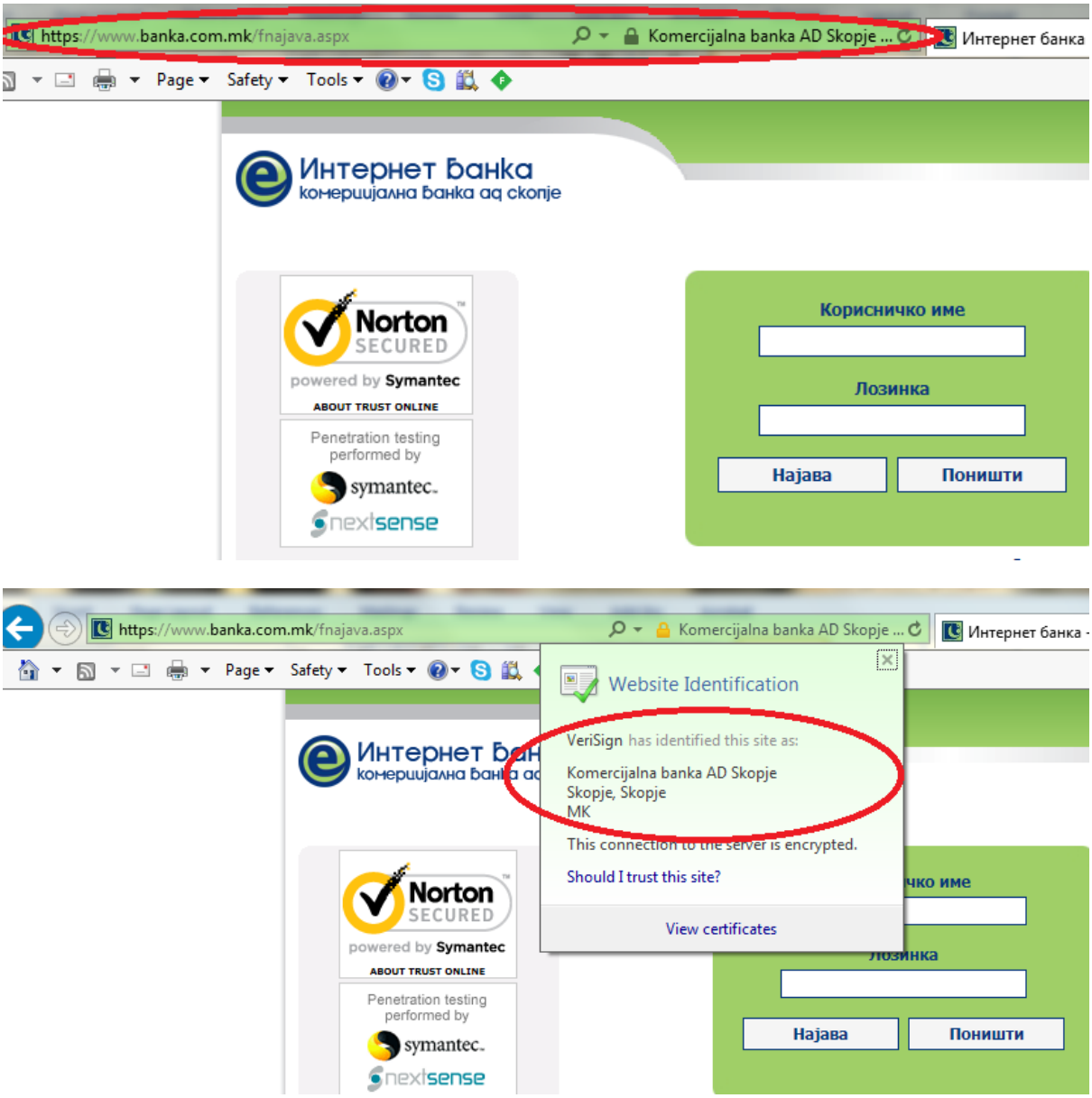
комерцијална банка ад скопје

Оваа порака и нејзините прилози може да содржат доверливи информации. Пораката не секогаш го изразува официјалниот став на Комерцијална банка АД Скопје. Пораката е проверена со антивирусен софтвер, но Банката не гарантира за неприсуството на злонамерен софтвер. Ако оваа порака не Ви е Вам наменета, Ве молиме да го информирате испраќачот и да ја избришете. Ако се сомневате во било каква злоупотреба, Ве молиме веднаш да не контактирате.

Доколку со покажувачот на глувчето се приближите до линкот ќе забележите дека истиот ве води на друга адреса различна од https://www.banka.com.mk (http://www.banka.com). Најчесто адресите на лажните (replica sites) web страни не се обезбедени со валиден серверски сертификат и користат обична некриптирана http конекција (криптираните се задолжително https) но тоа не мора да биде секогаш случај.

Жртвата која ќе кликне на линкот ќе биде насочена на сајт кој по својот изглед наликува на оригиналниот сајт на Банката но секако ја нема истата функционалност. Доколку малку подобро ги погледаме деталите во адресната лента, сепак разликите можат да се воочат:

Интернет банка на Комерцијална банка АД Скопје (обрнете внимание на бравата на која со кликнување се појавува потврдата дека сте поврзани на оригиналниот сајт)	Лажната копија на сајтот на Интернет банката со која се крадат корисничките сметки и лозинки (во случајот линкот е различен и недостасува иконата на бравата)



Доколку корисникот се обиде да се најави и ги проследи точното корисничкото име и лозинка на лажната копија на сајтот на Интернет банката, жртвата без да знае, му ги проследува своите дигитални белези на измамникот кој подоцна може истите да ги искористи се со цел неавторизирано да дојде до чувствителните финансиски информации на корисникот.

Риболов со помош на злонамерни додатоци на Интернет прегледувачот (Man in the middle of the browser attack)

Еден малку помодерен и пософистициран начин на "риболов" подразбира употреба на злонамерни додатоци за Интернет прегледувачот на корисникот (Internet Explorer, Firefox Mozilla, Google Chrome) кој најчесто корисникот го инсталира на својата работната станица како корисен додаток на својот Интернет прегледувач. Неретко се случува без знаење на корисникот при прегледувањето на дадена злонамерна страна користејќи ги интерните слабости на оперативниот систем и Интернет прегледувачот

овој додаток (**Plug-in**, **Add on**) да се инсталира без знаење и одобрување на корисникот.

Злонамерниот додаток го прислушува прегледувањето на Интернет страните и штом ќе детектира HTTPS конекција или маски за внес на корисничко име и лозинка во форма модален pop-up прозорец ја исфрла следнава порака:

We do not recognize the computer you are using.

To continue with Online Banking, please provide the information requested below.

Confirm Your Identity

Instructions: Provide your Card Security Code and as much additional security information as you can. Your entries must match the information on the account record and will be used solely to confirm your identity.

Card Number :

[ ]

Card Security Code (required): Turn to the BACK of your card and look in the white panel where you signed your card. Type the last 3 digits of the code.

[ ]

Expiration Date: month/year

[01 \/] / [2010 \/]

ATM PIN:

[ ]

[Continue]

Во позадината на новопојавениот прозорец навистина се наоѓа страната на Интернет банката но модалниот прозорец не е дел од истата. Злонамерниот програм ја користи довербата на корисникот во страната на Интернет банката и се обидува да го стави во заблуда дека податоците кои се бараат на новопојавената форма се дел од истата.

Секако доколку се анализира содржината на оваа форма за внес можат да се воочат повеќе нелогичности кои сугерираат дека се работи за обид за измама:

1. Пораката е напишана на англиски. Званичните обраќања на Банката кон нејзините корисници резиденти се прават на македонски.

2. Во пораката се инсистира на чувствителни податоци за "наводна" дополнителна идентификација. Сакаме да напоменеме дека во моментот Банката веќе врши двофакторска идентификација со вашата лозинка и листата

на кодови за една употреба или токен и PIN-от за пристап до истиот. Овие белези се сосема доволни Интернет банката да ве идентификува. Уште повеќе ***Банката никогаш нема да побара на нејзиниот сајт или во порака испратена преку електронска пошта да и ги доставите погоре наведените чувствителни податоци***.

Препораки:

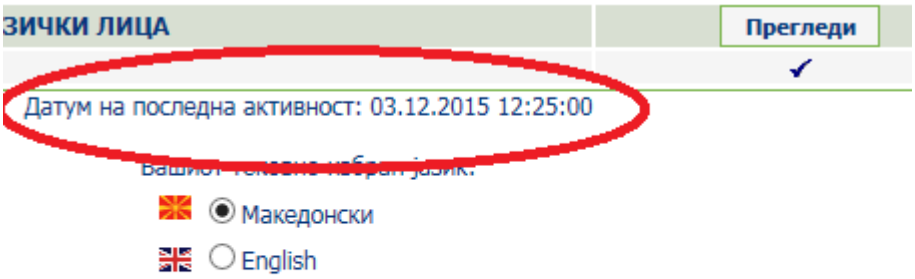
Никогаш не користете линкови од трети страни за да дојдете на сајтот на Интернет банката. Во Интернет прегледувачот внесете ја URL адресата https://www.banka.com.mk и од истата направете кратенка (shortcuts) или додадете ја во вашите омилени сајтови (Favorites). При наредната употреба кликнете на кратенката или линкот во Favorites. Секое друго одење на сајтот на Интернет банката преку линкови добиени по електронска пошта или изложени на трети сајтови независно дали се работи за Интернет весници, социјални сајтови (Facebook, MySpace), BLOG-ови и сл., во основа го носат ризикот да завршите во мрежата на измамниците и да станете жртва на кражба на вашиот дигитален идентитет.

Независно од авторитетот на страната со која во моментот комуницирате и начинот на кој таа комуникација ја воспоставувате (страната на Интернет банката, порака испратен по електронска пошта и сл.) не одговарајте и игнорирајте ги барањата за проследување на следните чувствителни информации:

- броеви на платежни картички
- PIN-от за авторизација на POS или банкомат
- сигурносниот 3-цифрен код на позадината на картичката со кој се авторизираат плаќањата за електронската трговија преку Интернет.
- вашиот ЕМБГ или други лични податоци кои се особено чувствителни и за кои Дирекцијата за заштита на лични податоци пропишала посебни стандарди за нивна заштита и евентуална размена.

Делувајте брзо и трезвено - разоткривање и постапки во случај на кражба на вашиот идентитетот

По секоја успешна најава во Интернет банката континуирано се регистрира времето на вашата последна активност . На страната на вашиот кориснички профил можете истото да го видите и да го споредите со вашите сознанија за последниот авторизиран пристап во Интернет банката:



Доколку забележите дата и време која не содејствува на вашиот последен пристап веднаш сменете ја вашата лозинка и пријавете го случајот во Help Desk-от на Интернет банката каде што врз основа на дневниците на активност ќе се разјаснат деталите за евентуалниот неовластен пристап до вашите финансиски информации.

Редовно проверувајте го вашиот извод и доколку забележите долговни ставки на вашиот извод за кои сте сигурни дека вие не сте ги авторизирале или не содејствуваат на набавените производи и услуги, веднаш обратете се до HelpDesk-от на Банката и побарајте понатамошни инструкции.

Во случај на губење на ливче на кое го имате евидентирано вашето корисничко име или лозинка, обидете се да се најавите во Интернет банката и веднаш сменете ја корисничката лозинка. Доколку не можете да се најавите во Интернет банката, случајот пријавете го во Help Desk-от и побарајте привремено блокирање на пристапот до Интернет банката од вашето корисничко име. По првото доаѓање во Банката и физичкото идентификување со валидна лична карта или патна исправа ќе ви биде издадена нова лозинка која потоа треба да ја смените и пристапот повторно до Интернет банката ќе ви би биде овозможен.

Во услови на губење или кражба на листата на кодови или сигурносниот токен, под итно пријавете го случајот во Help Desk-от на Банката и побарајте привремено блокирање на пристапот до Интернет банката од вашето корисничко име.

Во сите претходно наведени случаи особено суштински е работите да ги изведувате по следниот редослед:

- Контактирајте го Help Desk-от на Банката и по потреба побарајте привремено блокирање на пристапот до Интернет банката од вашето корисничко име.
- Дополнително по преземањето на претходно наведените заштитни мерки имате право случајот да го пријавите во МВР како и во Дирекцијата за заштита на лични податоци каде што по службена должност ќе се отпочне истрага против евентуалните сторители на делото.

Сигурносни пропусти и препораки за нивно избегнување

- Доколку сте најавени во Интернет банката никогаш не го оставајте вашиот компјутер отклучен и сигурносниот токен вметнат внатре во USB портата или на вашето биро листата со кодови за еднократна потреба. Доколку тоа го сторите на место каде што фреквентно поминуваат и други лица, на потенцијалниот измамник сте му ги оставиле сите врати отворени за пристап до вашите финансиски средства.
- ✓ Во услови кога привремено го напуштате вашиот компјутер задолжително направете негово заклучување (lock workstation) и со себе земете ја листата на кодови за еднократна употреба или сигурносниот токен. Имајте го во предвид фактот дека сигурносниот токен само еднаш го бара PIN-от за пристап до вашиот приватен клуч и дека истиот автоматски ќе ја одјави вашата сесија дури откако ќе поминат 15 – 20 минути на неактивност или доколку истиот го извлечете од USB портата.

- Никогаш не ја запишувајте вашата корисничка сметка и лозинка или PIN-от за пристап до дигиталниот сертификат на ливче сместено во вашиот паричник или во именикот на вашиот мобилен телефон. Праксата покажува дека најчесто се губат или се крадат токму паричниците и мобилните телефони.
- ✓ Доколку се плашите дека ќе ја заборавите лозинката или PIN-от истите можете да ги запишете на ливче кое ќе го чувате под клуч во вашето работно биро или во вашиот дом. Дополнително потрудете се работите да ги чувате на различни места се со цел со нивното губењето или кражба да не му овозможите на измамникот неавторизиран пристап.

- При изборот на лозинката никогаш не користете некоја од стандардните лозинки кои можат да се најдат во речникот на речиси било кој измамник (P@ssw0rd, admin, 1234567890, user, operator, Administrator, masterkey, sysadm, manager ….). Избегнувајте во составот на лозинката да користите цели поими, имиња или дати кои лесно можат да се доведат во врска со вашиот приватен живот (датата на раѓање на вашите деца, името на вашата сакана личност и сл.).
- ✓ Лозинката мора да има најмалку 8 карактери при што мора да се состои најмалку од три групи на карактери од следните четири по ваш слободен избор:

    - Мали букви
    - Големи букви
    - Цифри
    - Специјални знаци

- Еднаш зададената лозинка не ја користете повеќе од 90 дена. Дополнително не ја менувајте вашата лозинка повеќе пати последователно се со цел да го

заобиколите правилото според кое истата не треба да е дел од историјата на три последно користени лозинки.

- ✓ Се со цел полесно да ја запомните лозинката можете да си дефинирате ваше сопствено правило според кое ќе ги креирате идните лозинки.

- Не се најавувајте во Интернет банката на компјутер даден на јавно користење (пример: Интернет кафулиња) или компјутер кој го одржуваат непознати лица. Никогаш нема да бидете сигурни дека на погоре споменатите компјутери нема да налетате на притаени инсталации на злонамерни (malware) апликации кои ги крадат корисничките сметки и лозинки независно дали истите се здобиени заради непостоењето или лошата анти-вирусна заштита или можеби истите се со намера инсталирани од лицата кои ги одржуваат.
- ✓ Пристапот до Интернет банката правете го од својот сопствен преносен компјутер, компјутерот кој ви е доделен на користење на вашето работно место или вашиот домашен компјутер. Доколку сепак веќе сте се најавиле во Интернет банката од потенцијално несигурен и компромитиран компјутер, искористете ја првата можност и сменете ја вашата лозинка од вашиот домашен или вашиот личен преносен компјутер.

- Не го оставајте вашиот компјутер без редовно ажурирана анти-вирусна заштита и активен firewall. Избегнувајте инсталација на антивирус од непознат бренд бидејќи таквите апликации најчесто по инсталацијата лажно го алармираат корисникот за наводно откриен вирус и бараат доплата за негово целосно отстранување. Понекогаш таквите лажни анти-вирусни решенија дополнително можат да инсталираат злонамерни апликации (тројанци, spyware-и, key logger-и и слично) или да ве пренасочат на сајтови на кои е во тек риболовот...
- ✓ Пожелно е да користите анти-вирусната заштита од некој од попознатите брендови (Symantec, Nod32, Kaspersky, BitDefender, AVG, Panda, Avast) и изданието да биде целосен заштитен Интернет пакет во кој освен заштитата од вируси добивате и заштита од други типови на злонамерни програми (spyware, adware, тројанци), блокирање на злонамерни JavaScript-и при прегледувањето на Интернет страните, континуирано ажурирање на адресите на малициозните сајтови и нивно блокирање, двонасочна (outbound и inbound) firewall заштита и сл. Понекогаш соодветното комбинирање на повеќе заштитни софтверски пакети можат да дадат уште повисоко ниво на сигурност но при тоа треба да се внимава драстично да не го забавите вашиот компјутер и да не предизвикате конфликти помеѓу апликациите.

- Независно од оперативниот систем кој го користите, сурфањето со Интернет прегледувач за време на сесија во која сте најавени како привилегиран корисник (член на Local Administrators групата кај Windows платформата) е опасно.
- ✓ Неопходно е на вашиот компјутер да креирате корисничка сметка која не припаѓа на ниту една привилегирана корисничка група и истата да ја користите за време на сурфањето на Интернет а сесиите со привилегиран корисник да ги користите само по потреба кога сакате да инсталирате некоја нова апликација или вршите активности на периодично одржување на вашиот компјутер.

- Една од најлошите работи кои можете да ги сторите е да користите пиратска верзија на оперативен систем. Освен што користењето на вакви нелегални копии е казниво со закон дополнителен проблем е се почестата појава ваквите копии да се дистрибуираат со однапред инсталирани малициозни програми. Некои од нив (т.н. Rootkits) користат техники на невидливост и премостување на системските повици така што подоцна истите не можат да бидат откриени и отстранети со ниту една анти-вирусна апликација. Дополнително пиратскиот софтвер најчесто вклучува потреба од извршување на crack (апликација со која се разбива заштитата од нелиценцирано користење) со чија активација речиси редовно се здобивате со некоја нова софистицирана верзија на тројанец или Rootkit. Освен што ризикувате кражба на чувствителните информации и уништување на вашите документи, истовремено ризикувате вашиот искомпромитиран компјутер без ваше знаење да биде управуван далечински од разни криминални структури и истиот да биде искористен за активирање на DDoS (Distributed Denial of Service) напади врз сајтот на некоја компанија. Во таков случај вашата IP адреса ќе биде евидентирана како инкриминирачка при што ризикувате да бидете обвинети за евентуалната настаната штета.
- ✓ Користете лиценциран софтвер. Доколку вашите финансии тоа не ви го дозволуваат побарајте алтернатива во т.н. апликации со отворен код (open source).